CLAIMS

1. Method for matching digital data reception equipment (2) with a plurality of external security modules (6, 8) each with a unique identifier, method characterised in that it comprises the following steps:

- connecting an external security module (6, 8) to the reception equipment,
- memorising the unique identifier of the connected security module (6, 8) in the reception equipment (2), on the fly.

2. Method set forth in claim 1, characterised in that it also includes a check phase consisting of verifying whether or not the identifier of said module is memorised in reception equipment (2), every time that an external security module (6, 8) is connected to this reception equipment (2) later on.

3. Method set forth in claim 2, characterised in that it also comprises a step of transmitting a signal to the reception equipment (2) including at least one message to manage memorisation of the identifier of the external security module (6, 8) and/or a check phase management message.

4. Method set forth in claim 3, characterised in that said signal includes at least one of the following set values:

- authorise memorisation,
- prohibit memorisation,
- erase identifiers previously memorised in the reception equipment (2),
- activate or deactivating the check phase.

5. Method set forth in claim 3, characterised in that said signal also includes the maximum allowable number of memorised identifiers.

6. Method set forth in claim 3, characterised in that said signal includes a reconfiguration set value through which an updated list of identifiers of external security modules (6, 8) matched with the reception equipment(2) is transmitted to said reception equipment (2).

7. Method set forth in claim 6, characterised in that said list is transmitted directly to the reception equipment (2).

8. Method set forth in claim 6, characterised in that said list is transmitted through an external security module (6, 8) connected to said reception equipment (2).

9. Method set forth in claim 2, in which said check phase includes a procedure consisting of disturbing the data processing if the identifier of the connected external security module (6, 8) is not previously memorised in the reception equipment (2).

10. Method set forth in claim 1, characterised in that said data are distributed without encryption or scrambled by an encrypted control word and in that each external security module (6, 8) includes access rights to said data and a decryption algorithm for said control word.

11. Method set forth in one of claims 4 or 5, characterised in that said signal is transmitted to a reception equipment (2) in an EMM message specific to an external security module (6, 8) associated with this reception equipment (2).

12. Method set forth in one of claims 4 or 5, characterised in that said signal is transmitted to a reception equipment (2) in an EMM message specific to this reception equipment (2).

13. Method set forth in claim 6, characterised in that for a given reception equipment (2) said list is transmitted in an EMM message specific to a security module (6, 8) associated with this reception equipment (2).

14. Method set forth in claims 4 or 5, characterised in that said signal is transmitted to a group of reception equipment (2) in an EMM message specific to a group of external security modules (6, 8) associated with said reception equipment (2).

15. Method set forth in one of claims 4 or 5, characterised in that said signal is transmitted to a group of reception equipment (2) in an EMM message specific to said group of reception equipment (2).

16. Method set forth in claim 6, characterised in that for a given group of reception equipment (2), said list is transmitted in an EMM message specific to a group of external security modules (6, 8) associated with said reception equipment (2).

17. Method set forth in one of claims 4 or 5, characterised in that said check signal is transmitted in a private flow to a group of reception equipment (2).

18. Method set forth in claim 6, characterised in that for a given group of reception equipment (2), said list is transmitted in a private flow to each reception equipment (2).

19. Method set forth in one of claims 17 or 18, characterised in that said private flow is processed by a dedicated software executable in each reception equipment (2) as a function of the identifier of the external security module (6, 8) associated with it.

20. Method set forth in one of claims 11 to 16, characterised in that it also includes a mechanism that prevents the use of an EMM transmitted to the same security module (6, 8) in two distinct items of reception equipment (2).

21. Method set forth in one of claims 11 to 13, characterised in that said EMM are in the following format:

EMM-U_section() {	
table_id = 0x88	8 bits
section_syntax_indicator = 0	1 bit
DVB_reserved	1 bit
ISO_reserved	2 bits
EMM-U_section_length	12 bits
unique_adress_field	40 bits
for (i=0; i<N; i++) {	
EMM_data_byte	8 bits

22. Method set forth in one of claims 14 to 16, characterised in that said EMM is specific to all external security modules (6, 8) or to all reception equipment (2) and are in the following format:

EMM-G_section() {	
table_id = 0x8A or 0x8B	8 bits
section_syntax_indicator = 0	1 bit
DVB_reserved	1 bit
ISO_reserved 2 bits	
EMM-G_section_length	12 bits
for (i=0; i<N; i++) {	
EMM_data_byte	8 bits

23. Method set forth in one of claims 14 to 16, characterised in that said EMM is specific to a sub-group of external security modules (6, 8) or reception equipment (2) and are in the following format:

EMM-S_section() {	
table_id = 0x8E	8 bits
section_syntax_indicator = 0	1 bit
DVB_reserved	1 bit
ISO_reserved 2 bits	
EMM-S_section_length	12 bits
shared_address_field	24 bits
reserved	6 bits
data_format 1 bit	
ADF_scrambling_flag	1 bit
for (i=0; i<N; i++) {	
EMM_data_byte	8 bits

24. Method set forth in claim 1, characterised in that identifiers of external security modules (6, 8) are grouped in an encrypted list.

25. Method set forth in any one of claims 1 to 24, characterised in that the reception equipment (2) includes a decoder and the external security module (6, 8) includes an access control card (6) in which information about access rights of a subscriber to digital data distributed by an operator is memorised, and in that matching is done between said decoder and said card (6).

26. Method set forth in any one of claims 1 to 24, characterised in that the reception equipment (2) includes a decoder and the external security module (6, 8) includes a removable security interface (8) provided with a non-volatile memory that can cooperate firstly with the decoder, and secondly with a plurality of conditional access control cards (6) to manage access to digital data distributed by an operator, and in that matching is done between said decoder and said removable security interface (8).

27. Method set forth in any one of claims 1 to 24, characterised in that the reception equipment (2) includes a decoder provided with a removable security interface (8) with a non-volatile memory that can cooperate firstly with said decoder, and secondly with a plurality of conditional access control cards (6), and in that matching is done between said removable security interface (8) and said access control cards (6).

28. Method set forth in claim 10, characterised in that the data are audiovisual programs.

29. Reception equipment (2) that can be matched with a plurality of external security modules (6, 8) to manage access to digital data distributed by an operator, characterised in that it includes means of memorising the identifier of each external security module (6, 8) connected to it, on the fly.

30. Equipment set forth in claim 29, characterised in that it comprises a decoder and in that the external security module (6, 8) is an access control card (6) containing information about access rights of a subscriber to said digital data, matching being done between said decoder and said card (6).

31. Equipment set forth in claim 29, characterised in that it includes a decoder and in that the external security module (6, 8) is a removable security interface (8) provided with a non-volatile memory and that is designed to cooperate firstly with said decoder, and secondly with a plurality of conditional access control cards (6), to manage access to said digital data, matching being done between said decoder and said removable security interface (8).

32. Equipment set forth in claim 29, characterised in that it includes a decoder provided with a removable security interface (8) with a non-volatile

memory and that is designed to cooperate firstly with said decoder and secondly with a plurality of conditional access control cards (6) and in that matching is done between said removable security interface (8) and said access control cards (6).

33. Decoder that can cooperate with a plurality of external security modules (6, 8) to manage access to audiovisual programs distributed by an operator, each external security module (6, 8) having a unique identifier and including at least one data processing algorithm, decoder characterised in that it includes means of memorising the identifier of each external security module (6, 8) connected to it, on the fly.

34. Decoder set forth in claim 33, characterised in that said external security modules (6, 8) are access control cards (6) in which information about access rights of a subscriber to digital data distributed by an operator are stored.

35. Decoder set forth in claim 33, characterised in that said external security modules (6, 8) are removable security interfaces (8) including a non-volatile memory that can cooperate firstly with the decoder and secondly with a plurality of conditional access control cards (6) to manage access to digital data distributed by an operator.

36. Removable security interface (8) including a non-volatile memory and designed to cooperate firstly with a reception equipment (2), and secondly with a plurality of conditional access control cards (6), to manage access to digital data distributed by an operator, each card (6) having a unique identifier and containing information about access rights of a subscriber to said digital data, interface characterised in that it includes means of recording the identifier of each access control card (6) in said non-volatile memory, on the fly.

37. Interface set forth in claim 36, characterised in that it consists of a PCMCIA card on which digital data descrambling software is installed.

38. Interface set forth in claim 36, characterised in that it consists of a software module.

39. Executable computer program in a reception equipment (2) that can cooperate with a plurality of external security modules (6, 8) each having a unique identifier and in which information about access rights of a subscriber to digital data distributed by an operator are stored, characterised in that it includes instructions to memorise the identifier of each external security module (6, 8) connected to said reception equipment (2), on the fly.

40. Computer program set forth in claim 39, characterised in that it also includes instructions to locally generate matching control parameters of the reception equipment (2) with an external security module (6, 8) as a function of a signal transmitted to said reception equipment (2) by the operator.

41. Computer program set forth in claim 39, characterised in that it also includes instructions intended to check if the identifier of said external security module (6, 8) is memorised in the reception equipment (2), at each later use of an external security module (6, 8) with the reception equipment (2).

42. System including a plurality of reception equipment (2) connected to a data and/or services broadcasting network, each reception equipment (2) being capable of being matched with a plurality of external security modules (6, 8), said system also including a commercial management platform (1) communicating with the reception equipment (2) and with said external security modules (6, 8) characterised in that it also includes:

- a first module arranged in said commercial management platform (1) and that will generate matching queries,

- and a second security module arranged in said reception equipment (2) that will process said queries to prepare a matching configuration and to control matching.